gemeente Steenbergen

Rekenkamercommissie
Postbus 6
4650 AA STEEN-
BERGEN

Onderzoeksopzet ‘Privacy in de gemeente Steenbergen’

Inhoudsopgave

1. Aanleiding

Het opstellen van een jaarlijks onderzoeksprogramma door de Rekenkamercommissie Steenbergen (voortaan te noemen: RKC), gebeurt aan de hand van de 'Nota van werkwijze van de RKC Steenbergen'. Op basis van de in de Nota vastgelegde criteriakeuze, heeft de RKC haar afweging en keuze gemaakt om in de periode 1ste kwartaal 2021 – 3de kwartaal 2021 een onderzoek uit te voeren naar het onderwerp *Privacy in de gemeente Steenbergen*.

Dit voorliggend onderzoeksvoorstel geeft inzicht in:
- uitgangspunten en achtergronden van het onderzoek;
- de wijze waarop de RKC het onderzoek gaat uitvoeren.

2. Probleemanalyse

De verantwoordelijkheid van de gemeente Steenbergen op het gebied van privacy en informatiebeveiliging is de afgelopen jaren, mede door de komst van aanvullende wetgeving en nieuwe taken en samenwerkingsverbanden, enorm toegenomen.

Sinds 2015 zijn Nederlandse gemeenten verantwoordelijk geworden voor de diverse taken binnen het sociale domein zoals de Wet maatschappelijke ontwikkeling (WMO) en Jeugdwet. Voor deze taken werkt de gemeente Steenbergen onder meer samen met de gemeente Bergen op Zoom en gemeente Woensdrecht. De samenwerking is vastgelegd in Convenant Samenwerking Brabantse Wal en middels de Uitvoeringsagenda Samenwerking Brabantse Wal wordt de voortgang bewaakt.

Voor wat betreft aanvullende wetgeving valt te denken aan de Algemene Verordening Gegevensbescherming (AVG) per mei 2018 en Baseline Informatiebeveiliging Overheid (BIO) per mei 2019. In publicaties van de Autoriteit Persoonsgegevens (AP) na onderzoek onder Nederlandse gemeenten staat onder andere *"slechts enkele organisaties lijken duidelijke regels en of instructies te hebben ten aanzien van de wijze van registreren van datalekken"* en "het ontbreekt aan een heldere bepaling van wanneer en waarom toestemming wordt gevraagd bij de verwerking van persoonsgegevens in het sociaal domein" waaruit men kan concluderen dat gemeenten nog zoekende zijn om privacy goed te organiseren.

In de jaarrapportage gegevensbescherming van de gemeente (september 2019) wordt aangegeven dat de gemeentelijke organisatie niet aan de AVG voldoet doordat diverse systemen en werkprocessen daar niet volledig op ingericht zijn en dat het de nodige tijd zal vergen om volledig AVG-proof te werken. Verder dient de organisatie een risicoanalyse en optimalisatie van kwetsbare processen uit te voeren.

De bevindingen van de Autoriteit Persoonsgegevens, de status van de gemeentelijke organisatie t.a.v. de AVG en nieuwe taken voor kwetsbare inwoners van de gemeente zijn voor de Rekenkamer reden geweest om een onderzoek uit te voeren naar privacy binnen de gemeente Steenbergen.

3. Doelstelling

De RKC beoogt met dit onderzoek de gemeenteraad inzicht de geven in de mate van doeltreffendheid en doelmatigheid van het privacybeleid en de informatieveiligheid binnen de gemeente Steenbergen.

Met het onderzoek wil de RKC mogelijke richtingen van verbetering benoemen. Het onderzoek beoordeelt of de gemeentelijke kaders voldoen aan de landelijke wetgeving; in hoeverre de gemeentelijke kaders verwerkt zijn in de organisatie en werkprocessen; of de kaders als werkbaar worden ervaren; en op welke wijze de gemeenteraad betrokken is bij privacy en informatieveiligheid.

3.1 Vraagstelling

De centrale vraag van het onderzoek luidt als volgt: *In hoeverre zijn het privacybeleid en de informatieveiligheid van de gemeente Steenbergen doeltreffend en doelmatig?*

3.2 Deelvragen

De centrale vraag is uitgewerkt in de volgende 6 deelvragen:

1. Welke (wettelijke) kaders, doelstellingen en werkwijzen zijn van toepassing of zijn door de gemeente zelf geformuleerd op het gebied van informatiebeveiliging en privacy?
2. Hoe is de organisatie (ofwel: governance) van het privacybeleid en informatieveiligheid vormgegeven?
3. In welke mate zijn de gestelde kaders, doelstellingen en werkwijzen geborgd in de dagelijkse uitvoering?
4. Voldoet de gemeente Steenbergen op dit moment aan alle relevante wet- en regelgeving t.a.v. informatiebeveiliging en privacy?
5. Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers van de gemeente Steenbergen t.a.v. informatieveiligheid en privacy?
6. Op welke wijze is de gemeenteraad betrokken bij het stellen van kaders en het formuleren van doelen t.a.v. informatiebeveiliging en privacy? En hoe oefent zij haar controlerende functie op dit onderwerp uit?

3.3 Afbakening

De volgende onderdelen bepalen de afbakening van het onderzoek:

- Het onderzoek richt zich in principe op de periode vanaf 2018
- De deelvragen 1 t/m 6 beantwoordt de RKC op basis van documentonderzoek, andere relevante informatie en interviews met de verantwoordelijk portefeuillehouder(s), gemeenteambtenaren en mogelijk ook raadsleden.
- Het is mogelijk dat de RKC ten aanzien van deelvragen 3 en 6 een enquête uitvoert onder ambtenaren van de gemeente.

4. Formulering beleidstheorie

In de probleemanalyse is omschreven dat de verantwoordelijkheid van de gemeente Steenbergen t.a.v. privacy en informatiebeveiliging enorm is toegenomen. Dit mede door de introductie van nieuwe of aanvullende wetgeving.

Doel van dit onderzoek is toetsen in hoeverre de gemeente Steenbergen voldoet aan deze wetgeving (compliance) en hoe dit is geborgd (governance) in de organisatie.

Vaak geldt dat organisaties niet aan alle bepalingen kunnen voldoen, maar dat er sprake is van een “comply or explain” (pas toe of leg uit) principe. Dat wil zeggen dat organisatie als ze besluiten om iets niet te doen zij wel uit moeten leggen waarom niet. Ook dit wordt getoetst als onderzoek van het onderzoek.

5. Definitie begrippen

Privacy en informatiebeveiliging zijn twee nauw verbonden begrippen. Privacy gaat over de verzameling van persoonsgegevens, doelbinding en gebruik, toegang tot persoonsgegevens en gegevenskwaliteit. Informatiebeveiliging gaat over de beschikbaarheid van data en systemen, integriteit en vertrouwelijkheid. Op het snijvlak van privacy en informatiebeveiliging moeten afspraken worden gemaakt over het beveiligingsbeleid, de toegangscontrole, fysieke beveiliging alsmede de beschikbaarheid en de naleving van data en systemen.

De gemeentelijke organisatie moet werken volgens diverse (internationale) wetten t.a.v. privacy en informatieveiligheid: Wet digitale overheid (WDO), Wet modernisering elektronisch bestuurlijk verkeer (MEBV), Algemene verordening gegevensbescherming (AVG), Uitvoeringswet algemene verordening gegevensbescherming (UAVG), Wet basisregistratie personen (BRP).

Daarnaast is vanaf 1 januari 2020 de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Van BIG, BIR, BIR2017, IBI en BIWA naar BIO. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. De BIO beschrijft de invulling van de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 voor de overheid.

6. Operationalisering

De gebruikte onderzoeksmethoden voor de beantwoording van de zes deelvragen staan in onderstaande Tabel 1 beschreven.

Deelvraag	**Onderzoeksmethoden**		
	Documentenanalyse	**Interviews**	**Enquête**
1. Welke (wettelijke) kaders, doelstellingen en werkwijzen zijn van toepassing of zijn door de gemeente zelf geformuleerd op het gebied van informatiebeveiliging en privacy?	• Jaarrapportages gegevensbescherming vanaf 2018 • Privacybeleid en privacyverklaring • Uitvoeringsdocumenten en procesbeschrijvingen	• Bestuurlijk verantwoordelijken • Ambtelijk verantwoordelijken	
2. Hoe is de organisatie (ofwel: governance) van het privacy beleid en informatieveiligheid vormgegeven?	• Jaarrapportages gegevensbescherming vanaf 2018 • Uitvoeringsdocumenten en procesbeschrijvingen	• Bestuurlijk verantwoordelijken • Ambtelijk verantwoordelijken	
3. In welke mate zijn de gestelde kaders, doelstellingen en werkwijzen geborgd in de dagelijkse uitvoering?	• Jaarrapportages gegevensbescherming vanaf 2018 • Uitvoeringsdocumenten en procesbeschrijvingen	• Bestuurlijk verantwoordelijken • Ambtelijk verantwoordelijken	• Mogelijkerwijze een enquête uitzetten onder ambtenaren
4. Voldoet de gemeente Steenbergen op dit moment aan alle relevante wet- en regelgeving t.a.v. privacy en informatiebeveiliging?	• Jaarrapportages gegevensbescherming vanaf 2018 • Uitvoeringsdocumenten en procesbeschrijvingen	• Bestuurlijk verantwoordelijken • Ambtelijk verantwoordelijken	
5. Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers van de gemeente Steenbergen t.a.v. informatieveiligheid en privacy?	• Jaarrapportages gegevensbescherming vanaf 2018 • Uitvoeringsdocumenten en procesbeschrijvingen	• Bestuurlijk verantwoordelijken • Ambtelijk verantwoordelijken	
6. Op welke wijze is de gemeenteraad betrokken bij het stellen van kaders en het formuleren van doelen t.a.v. informatiebeveiliging en privacy? En hoe oefent zij haar controlerende functie op dit onderwerp uit?	• Jaarrapportages gegevensbescherming vanaf 2018 • Betreffende jaarverslagen en raadsvoorstellen	• Bestuurlijk verantwoordelijken • Ambtelijk verantwoordelijken	• Mogelijkerwijze een enquête uitzetten onder ambtenaren en raadsleden?

Tabel 1: Operationalisering

7. Normen c.q. normering

Om een afgewogen en objectief onderzoek tot stand te brengen, is het belangrijk om de gevonden onderzoeksuitkomsten te 'confronteren' met vooraf gestelde normen ofwel beoordelingscriteria. De in dit onderzoek geformuleerde normen staan per deelvraag weergegeven in Tabel 2.

Deelvraag	Normen/beoordelingscriteria
1. Welke (wettelijke) kaders, doelstellingen en werkwijzen zijn van toepassing of zijn door de gemeente zelf geformuleerd op het gebied van informatiebeveiliging en privacy?	• Er wordt een overzicht gemaakt van welke kaders, werkwijzen en doelstellingen die gemeente toepast.
2. Hoe is de organisatie (ofwel: governance) van het privacybeleid en informatieveiligheid vormgegeven?	• Wat is het beleid en wie is verantwoordelijk?
3. In welke mate zijn de gestelde kaders, doelstellingen en werkwijzen geborgd in de dagelijkse uitvoering?	• De doelstellingen op het gebied van privacy zijn inzichtelijk en SMART geformuleerd. • De doelstellingen en werkwijzen op het gebied van privacy sluiten logisch aan op relevante wetgeving
4. Voldoet de gemeente Steenbergen op dit moment aan alle relevante wet- en regelgeving t.a.v. privacy en informatiebeveiliging?	• De gemeente is compliant met relevante wetgeving t.a.v. privacy en informatieveiligheid • De gemeente heeft een nulmeting op de BIO uitgevoerd, een GAP analyse gemaakt en de noodzakelijke maatregelen geimplementeerd • De systemen met vertrouwelijke informatie voldoen aan het BIO BBN2 beveiligingsniveau
5. Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers van de gemeente Steenbergen t.a.v. informatieveiligheid en privacy?	• Er wordt aandacht besteed aan awareness onder medewerkers d.m.v. trainingen, campagnes en steekproeven • Nieuwe medewerkers worden vroegtijdig meegenomen in de relevante procedures en werkwijzen • De ingezette instrumenten hebben geleid tot het realiseren van meer awareness rondom privacy
6. Op welke wijze is de gemeenteraad betrokken bij het stellen van kaders en het formuleren van doelen t.a.v. informatiebeveiliging en privacy? En hoe oefent zij haar controlerende functie op dit onderwerp uit?	• De gemeenteraad wordt periodiek – bijv. twee keer per jaar – geïnformeerd door het college • De gemeenteraad wordt periodiek – bijv. twee keer per jaar – voorzien van een rapportage waarin is toegelicht in welke mate de ambtelijke organisatie voldoet aan de privacy wetgeving.

Tabel 2: Normenkader

8. Keuze type onderzoek

Een beschrijvend/verkennend onderzoek a.d.h.v. de jaarrapportage gegevensbescherming gemeente Steenbergen naar de stand van zaken aangaande Privacy binnen de Gemeente Steenbergen.

9. Selectie van onderzoeksobjecten/organisaties t.b.v. het onderzoek Privacy

1. Inwoners; n.v.t.
2. Bedrijven; n.v.t.
3. Ambtelijke vertegenwoordigers, gemeente Steenbergen waaronder:
    a. Chief Information Security Officer (CISO)
    b. Functionaris gegevensbescherming (FG)
    c. Personeel & Organisatie
    d. Algemene dienstverlening & Burgerzaken
    e. ICT
    f. WMO en/of Jeugdzorg
4. Portefeuillehouders
    a. Portefeuillehouder Financiën, Personeel & Organisatie, WMO & Jeugdzorg (wethouder Krook)
    b. Portefeuillehouder Algemene dienstverlening en Burgerzaken, ICT (wethouder Prent)

5. Raadsleden (selectie van raadsleden)

10. Gegevensverzameling en -verwerking

Voor het onderzoek zal gebruik gemaakt worden van:

- Deskresearch; documentanalyse van relevante beleids- en verantwoordingsstukken.
- (Diepte) interviews; met betrekking tot de rol van ketenpartners de samenhang tussen instrumenten en gemeentelijke ambities.
- Data-analyse; kwantitatieve gegevens over de (ontwikkeling) van de indicatoren en doelrealisatie.
- (Digitale) enquête; een (digitale) enquête wordt ingezet om de status van de dagelijkse uitvoering en bewustwording te meten.

11. Oordeel over uitbesteden van het onderzoek

De RKC heeft in 2017 besloten om zelf onderzoeken uit te voeren, en hierdoor is het uitgangspunt om niet uit te besteden. Echter, indien gedurende het onderzoek blijkt dat toch onverhoopt ondersteuning nodig is voor bepaalde onderdelen/onderwerpen van het onderzoek, dan zal alsnog gebruik gemaakt worden van uitbesteden.

12. Conceptbegroting, tijdsduur en opleveren eindrapport

De onderstaande Tabel 3 geeft een globaal inzicht in de conceptbegroting, de geplande werkzaamheden met bijhorende urenraming, en periode van oplevering van het eindrapport.

Onderzoekfase	**Uit te voeren werkzaamheden**	**Uren raming**	**Kosten-raming**	**Realisatie van de uren + korte toelichting op de werkzaamheden**
a) Verzamelen en ordenen van de gegevens	- Informatie opvragen en bestuderen van relevante (beleid)documenten. - Voorbereiden en afnemen interviews met de verantwoordelijk portefeuillehouder en (beleid)ambtenaren. - Voorbereiden van interviews met burgers die betrokken zijn of zijn geweest in duurzaamheidsprojecten. - Afnemen interviews met burgers die betrokken zijn of zijn geweest in duurzaamheidsprojecten. - Hoor en wederhoor toepassen, en verwerken interviews. - Voorbereiden en opstellen van vragen voor een uit te voeren enquête. - Uitvoeren en verwerken van een enquête.	160	€ 10.400,-	
b) Analyseren van de gegevens.	- Systematisch classificeren van de gegevens. - Het toepassen van (statistische) technieken op de gegevens. - Verbanden opsporen en toetsen.	60	€ 3.900,-	

	- Interpreteren van de analyse-gegevens in het kader van de onderzoeksvragen.			
c) Samenstellen van het onderzoeksrapport	- Teksten schrijven, opmaken van de inhoud en redigeren.	40	€ 2.600,-	
TOTAAL		260	€ 16.900,-	
Eindrapport gereed:		3de kwartaal 2021		

Tabel 3: Conceptbegroting, urenraming en oplevering

13. Planning op hoofdlijnen

Onderdeel	Datum bespreken/gereed	Uit te voeren door	Status
Onderzoeksvoorstel Privacy versie 0.1 bespreken in RKC vergadering	8 december 2020, bespreken	Gehele RKC	
Definitief versie onderzoeksvoorstel privacy opstellen	6 januari 2021, bespreken	Gehele RKC	
Definitief vaststellen van het onderzoekvoorstel privacy	20 januari 2021, gereed	Gehele RKC	
Aanbieden per brief van het onderzoeksvoorstel privacy aan de Gemeenteraad en het College	14 februari 2021, gereed	Secretaris RKC	
Start onderzoek privacy	15 februari 2021	Gehele RKC	
Deskstudie, afnemen interviews, interview verslagen uitwerken, onderzoekdata analyseren	15 februari 2021 – 14 juni 2021	Gehele RKC	
Samenstellen van het onderzoeksrapport privacy	15 juni – 14 september 2021	Gehele RKC	
Onderzoeksrapport privacy aanbieden aan het college en de gemeenteraad	1 november 2021, gereed	Gehele RKC	

Tabel 4: Planning op hoofdlijnen

De uitvoering en afstemming van de planning gebeurt gedurende het gehele onderzoek in overleg tussen de RKC, de concerncontroller en de Griffie van de gemeente Steenbergen.

Lijst van Tabellen

Gebruikte bronnen

- Het ontwerpen van een onderzoek, P. Verschuren en H. Doorewaard, 2015
- Organisatieonderzoek, A.H. van der Zwaan, 2003
- Website gemeente Steenbergen
- Raadsmededeling rapportage privacy gemeente Steenbergen (BM1905142)
- Jaarrapportage gegevensbescherming gemeente Steenbergen (BM1905568)
- Wet digitale overheid (WDO); https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/

- Wet modernisering elektronisch bestuurlijk verkeer (MEBV); https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-modernisering-elektronisch-bestuurlijk-verkeer/
- Algemene verordening gegevensbescherming (AVG); https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679
- Uitvoeringswet algemene verordening gegevensbescherming (UAVG); https://wetten.overheid.nl/BWBR0040940/2020-01-01
- Wet basisregistratie personen (BRP); https://wetten.overheid.nl/BWBR0033715/2019-02-03
- Privacyverklaring gemeente Steenbergen; https://www.gemeente-steenbergen.nl/privacy_verklaring/
- Privacybeleid gemeente Steenbergen; https://organisatie.gemeente-steenbergen.nl/overzicht_organisatie/gemeentelijke_regelgeving/algemeen_privacybeleid_gemeente_steenbergen/
- Baseline Informatiebeveiliging Overheid (BIO); https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/
- Raadsvoorstel Convenant Samenwerking Brabantse Wal (BM1703290); https://raad.gemeente-steenbergen.nl/Vergaderingen/Oordeelvormende-vergadering/2017/04-oktober/19:30/Raadsvoorstel-Convenant-Samenwerking-Brabantse-Wal-2017-BM1703290.pdf
- Ontwerp convenant Samenwerking Brabantse Wal; https://raad.gemeente-steenbergen.nl/Vergaderingen/Oordeelvormende-vergadering/2017/04-oktober/19:30/Bijlage-Ontwerp-convenant-Samenwerking-Brabantse-Wal-BBM1701321.pdf
- AP doet handreikingen om registratie datalekken te verbeteren; https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handreiking_verbeteren_registratie_datalekken.pdf
- Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming; https://autoriteitpersoonsgegevens.nl/sites/default/files/01_rapport_de_rol_van_toestemming_in_het_sociaal_domein.pdf